ARITHMETIC UNIT AND CRYPTOGRAM PROCESSOR

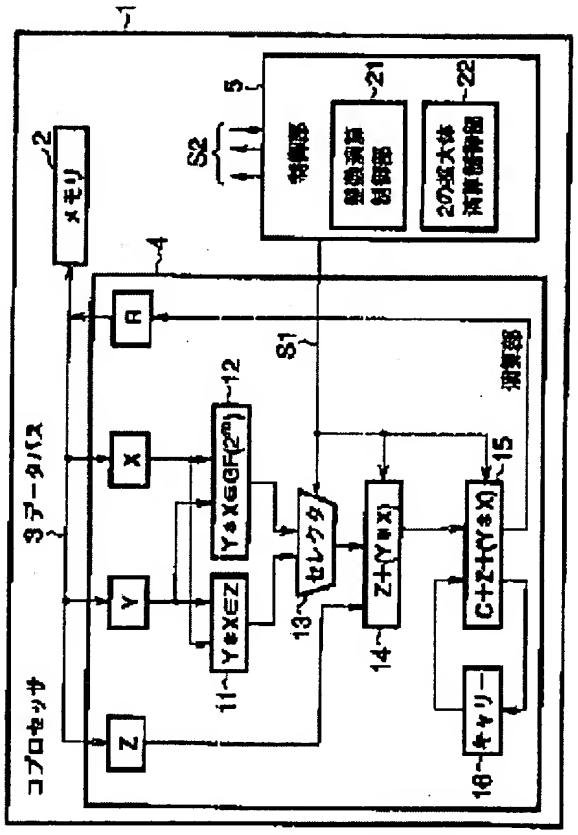
Patent number:	JP2001034167
Publication date:	2001-02-09
Inventor:	SHIBA KAZUE; KAWAMURA SHINICHI
Applicant:	TOSHIBA CORP
Classification:	
- international:	G09C1/00; G06F7/00; G06F12/14; G06K19/07
- european:	
Application number:	JP19990209831 19990723
Priority number(s):	

Report a data error here

Abstract of **JP2001034167**

PROBLEM TO BE SOLVED: To enable arithmetic operation to be executed without remaking a device main body even when the extension order of an extension field of 2 is increased by providing a control means for executing remainder multiplication in a product sum arithmetic circuit after dividing remainder multiplication into multiplication processing and remainder calculation processing.

SOLUTION: The arithmetic unit having product sum arithmetic circuits 12, 14, 15 of multiple length is provided with a control part 5 for executing remainder multiplication in the product sum arithmetic circuits 12, 14, 15 after dividing remainder multiplication into multiplication processing and remainder calculation processing. A multiplication circuit 12 on the extension field of 2 executes a part of multiplication on the extension field of 2 by data X in a buffer X and data Y in a buffer Y and outputs result to a selector 13. The selector 13 outputs either output from an integer type multiplication circuit 11 or output from the multiplication circuit 12 on the extension field of 2 to an adding circuit 14 according to a signal S1 from the control part 5. The adding circuit 14 is composed of a full adder which adds data z in a buffer Z to selector output and outputs the result to an adding circuit 15.



Reference Number:

Mailing Number: 164031

Mailing Date: May 10, 2005

TRANSLATION OF NOTICE OF REASONS FOR REFUSAL

Patent Application No. 2002-566769

Date Drafted: April 27, 2005

Examiner: Shinichi YAMASAKI 9174 5E00

Attorney: Kenzo HARA (and two other attorneys)

Provisions Applied: the first sentence of Section 29, Section 29(2), and Section 36

This application is refused for the reasons set forth below. If the applicant has any comments on this Office Action, a response should be filed within 3 months from the mailing date of this Action.

Reasons for Refusal

A. The inventions in the claims listed below of the present application should not comply with the requirements under the first sentence of Section 29(1).

Remarks

- Claims: 1 through 6
- Note:

Claims 1 through 6 are unclear as to what operates, and are merely arbitrary arrangements.

The present invention according to claims 1 through 6 is not obviously industrially applicable invention under the first sentence of Section 29(1). Thus, the Examiner does not examine the invention on some requirements for patentability, such as novelty and inventive step, of the present invention.

B. The inventions in the claims listed below of the present application should not be granted a patent under the provision of Patent Law Section 29(2) since they could have easily been made by persons who have common knowledge in the technical field to which the inventions pertain, on the basis of the inventions described in the publications listed below which were distributed in Japan or foreign countries prior to the filing of the present application.

Remarks (See the List of References Cited for the references cited herein)

- Claims: 7 through 13
- Cited References: 1 and 2
- Note:

Reference 2 describes that calculation is performed by using an intermediate result polynomial in a multiplication circuit on finite field. By arranging the circuit described in Reference 1 to use the arrangement of Reference 2 for the multiplication circuit on finite field, the person skill in the art can easily arrive at the present invention.

C. The claims listed below do not comply with the requirements under Patent Law Section 36(6)(ii).

Remarks

- Claims: 7 through 13

(1) It is unclear what are meant by "a multiplication look-ahead method" and "a reduction look-ahead method".

(2) Following Japanese expression "means ... reduction shift value (S_N) being equal to the difference of the degree of said shifted intermediate result polynomial (Z) and the degree of said modulus polynomial (N)" is unclear.

Therefore, the present invention according to claim 7 and its dependent claims 8 through 13 is unclear.

If any reasons for refusal are found later, it will be notified.

References Cited

1. Japanese Laid-Open Patent Application No. 018387/1988 (Tokukaisho 63-018387)
2. Japanese Laid-Open Patent Application No. 212951/1999 (Tokukaihei 11-212951)

Search Report for Prior Art Documents

Field of Search: IPC(7) G06F 7/72

DB-names

Prior Art Documents

Japanese Laid-Open Patent Application

No. 034167/2001 (Tokukai 2001-034167)

This search report does not constitute reasons for refusal.

Any inquiry concerning this Reasons for Refusal or a request for an interview should be directed to:

Shinichi YAMASAKI
Examiner Unit for Interface
Patent Examination Department 4
Tel: 03-3581-1101 (ext. 3520)
Fax: 03-3580-6907